

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-141916
(43)Date of publication of application : 17.05.2002

(51)Int.Cl. H04L 12/28
H04L 12/44

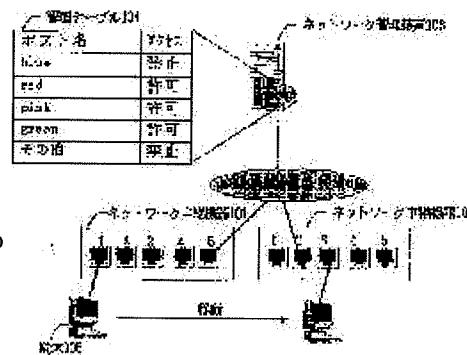
(21)Application number : 2000-337266 (71)Applicant : HITACHI CABLE LTD
(22)Date of filing : 31.10.2000 (72)Inventor : HIRAOKA DAIKI

(54) NETWORK MANAGEMENT SYSTEM, AND NETWORK REPEATER AND NETWORK MANAGEMENT DEVICE USED FOR THE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network management system ensuring the security, and a network repeater and a network management device used for the system.

SOLUTION: The network repeater 101 transmits information of a terminal 105 connected to the repeater 101 to the network management device 103, which returns information denoting an access permission/inhibition to the network repeater 101 depending on the terminal information, and the network repeater 101 sets use permission/use inhibit to a port to which the terminal 105 is connected based on the access permission/inhibition information. Since the permission/inhibition of the port to which the terminal 105 is connected is set depending on the terminal information managed by the network management device 103, the security is ensured without disturbing the use of a legal terminal.



* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

[Claim(s)]

[Claim 1]Information on a terminal connected from network relay apparatus is transmitted to a network management device, Information the network management device indicates an access permit/prohibition to be according to said terminal information is replied to said network relay apparatus, A network management system setting up a port where said network relay apparatus has connected a terminal based on said access permit/inhibition information improper [usable/use].

[Claim 2]The network management system according to claim 1, wherein said terminal information is the identification information of a user who is using the terminal concerned.

[Claim 3]The network management system according to claim 1, wherein said terminal information is a host name of the terminal concerned.

[Claim 4]The network management system according to claim 1, wherein said terminal information is an IP address of the terminal concerned.

[Claim 5]The network management system according to claim 1, wherein said terminal information is a MAC Address of the terminal concerned.

[Claim 6]Network relay apparatus provided with a function which transmits information on a terminal connected to a network management device in network relay apparatus.

[Claim 7]When information which shows an access permit/prohibition from said network management device as a reply to transmission of said terminal information is received, The network relay apparatus according to claim 6 provided with a function to set up a port which has connected a terminal based on this access permit/inhibition information improper [usable/use].

[Claim 8]The network relay apparatus according to claim 6 or 7 provided with a

function which can perform setting out in a port which transmits said terminal information to a network management device, and a port which does not transmit said terminal information to a network management device for every port.

[Claim 9]The network relay apparatus according to claim 8 provided with a function in which use propriety of a port can be arbitrarily set up to a port which does not transmit said terminal information to a network management device.

[Claim 10]claims 6–9 provided with a function in which it can be specified to which network management device said terminal information is transmitted -- either -- network relay apparatus of a statement.

[Claim 11]claims 6–10 having a function which use propriety of a port where a terminal is connected can set up beforehand when there is no reply from said network management device to transmission of said terminal information -- either -- network relay apparatus of a statement.

[Claim 12]claims 6–11, wherein said terminal information is the identification information of a user who is using the terminal concerned acquired from the contents of data which the terminal concerned transmits -- either -- network relay apparatus of a statement.

[Claim 13]As for said terminal information, claims 6–11 being the host names of the terminal concerned acquired from the contents of data which the terminal concerned transmits are network relay apparatus of a statement either.

[Claim 14]claims 6–11, wherein said terminal information is an IP address of the terminal concerned acquired from the contents of data which the terminal concerned transmits -- either -- network relay apparatus of a statement.

[Claim 15]claims 6–11, wherein said terminal information is a MAC Address of the terminal concerned acquired from the contents of data which the terminal concerned transmits -- either -- network relay apparatus of a statement.

[Claim 16]A network management device characterized by having a function to reply information which shows an access permit/prohibition according to said terminal information to said network relay apparatus when information on a terminal is received from network relay apparatus in a network management device.

[Claim 17]The network management device according to claim 16 provided with a function in which correspondence with information which shows the access permit/prohibition which should be replied to said network relay apparatus, and said terminal information is manageable.

[Claim 18]The network management device according to claim 16 or 17, wherein said terminal information is the identification information of a user who is using the

terminal concerned.

[Claim 19]The network management device according to claim 16 or 17, wherein said terminal information is a host name of the terminal concerned.

[Claim 20]The network management device according to claim 16 or 17, wherein said terminal information is an IP address of the terminal concerned.

[Claim 21]The network management device according to claim 16 or 17, wherein said terminal information is a MAC Address of the terminal concerned.

[Claim 22]IP subnet which specifies two or more IP addresses by making an IP address and an effective-bits mask value into a group is used, The network management device according to claim 20 provided with a function to define correspondence with this IP subnet, and an access permit/inhibition information, and to manage correspondence with said access permit/inhibition information, and an IP address of said terminal in the light of this definition.

[Claim 23]claims 16–22 provided with a function in which the contents of transmission from said network relay apparatus and the reply to that transmission are recorded as a log, and this log can be referred to from a management screen — either — a network management device of a statement.

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the network management system which used network relay apparatus, and relates to the network relay apparatus and the network management device which are used for the network management system and it which can secure security especially.

[0002]

[Description of the Prior Art]Many network relay apparatus is provided with the setting up function of the use propriety of a port. If a port is set up improper [use], the network equipment connected to the port cannot communicate via said network relay apparatus.

[0003]

[Problem(s) to be Solved by the Invention]If the port is set up usable even if it connects which terminal to the network relay apparatus currently installed on the network, the terminal can communicate via said network relay apparatus. Temporarily, it can communicate similarly at the terminal of the invader from the outside with bad faith. If a port is set up improper [use] so that an invader's terminal cannot access a network, the terminal in which a network should be essentially allowed access is also made to access a network. Thus, in the network management system using

conventional network relay apparatus, reservation of security is difficult.

[0004]Then, the purpose of this invention solves an aforementioned problem and there is in providing the network relay apparatus and the network management device which are used for the network management system and it which can secure security.

[0005]

[Means for Solving the Problem]To achieve the above objects, a network management device of this invention, Information on a terminal connected from network relay apparatus is transmitted to a network management device, Information the network management device indicates an access permit/prohibition to be according to said terminal information is replied to said network relay apparatus, and a port where said network relay apparatus has connected a terminal based on said access permit/inhibition information is set up improper [usable/use].

[0006]Said terminal information may be the identification information of a user who is using the terminal concerned.

[0007]Said terminal information may be a host name of the terminal concerned.

[0008]Said terminal information may be an IP address of the terminal concerned.

[0009]Said terminal information may be a MAC Address of the terminal concerned.

[0010]Network relay apparatus of this invention is provided with a function which transmits information on a terminal connected to a network management device.

[0011]When information which shows an access permit/prohibition from said network management device as a reply to transmission of said terminal information is received, it may have a function to set up a port which has connected a terminal based on this access permit/inhibition information improper [usable/use].

[0012]It may have a function which can perform setting out in a port which transmits said terminal information to a network management device, and a port which does not transmit said terminal information to a network management device for every port.

[0013]It may have a function which use propriety of a port can set up arbitrarily to a port which does not transmit said terminal information to a network management device.

[0014]It may have a function in which it can be specified to which network management device said terminal information is transmitted.

[0015]When there is no reply from said network management device to transmission of said terminal information, it may have a function which use propriety of a port where a terminal is connected can set up beforehand.

[0016]Said terminal information may be the identification information of a user who is using the terminal concerned acquired from the contents of data which the terminal

concerned transmits.

[0017]Said terminal information may be a host name of the terminal concerned acquired from the contents of data which the terminal concerned transmits.

[0018]Said terminal information may be an IP address of the terminal concerned acquired from the contents of data which the terminal concerned transmits.

[0019]Said terminal information may be a MAC Address of the terminal concerned acquired from the contents of data which the terminal concerned transmits.

[0020]A network management device of this invention is provided with a function to reply information which shows an access permit/prohibition according to said terminal information to said network relay apparatus when information on a terminal is received from network relay apparatus.

[0021]It may have a function in which correspondence with information which shows the access permit/prohibition which should be replied to said network relay apparatus, and said terminal information is manageable.

[0022]Said terminal information may be the identification information of a user who is using the terminal concerned.

[0023]Said terminal information may be a host name of the terminal concerned.

[0024]Said terminal information may be an IP address of the terminal concerned.

[0025]Said terminal information may be a MAC Address of the terminal concerned.

[0026]IP subnet which specifies two or more IP addresses by making an IP address and an effective-bits mask value into a group is used, Correspondence with this IP subnet, and an access permit/inhibition information is defined, and it may have a function to manage correspondence with said access permit/inhibition information, and an IP address of said terminal in the light of this definition.

[0027]The contents of transmission from said network relay apparatus and the reply to that transmission may be recorded as a log, and it may have a function in which this log can be referred to from a management screen.

[0028]

[Embodiment of the Invention]Hereafter, the embodiment of this invention is explained in full detail based on an accompanying drawing.

[0029]1) As shown in the first embodiment drawing 1, the network management system concerning this invention is provided with the following.

Two sets of network relay apparatus 101,102 concerning this invention.

The network management device 103 concerning this invention.

Network relay apparatus is a switching hub, for example.

[0030]As shown in drawing 2, the switching hub 201 comprises No. 1 – the No. 5 ports

202-206, the junction circuit 207, the processor 208, and memory 209 grade.

[0031]The processing which an administrator performs to below to the processing and network relay apparatus which the network relay apparatus of switching hub 201 grade performs is shown.

[0032](1) Beforehand, the administrator sets up whether the information on the terminal is transmitted to a network management device, when a terminal is connected for every port. The port which transmits terminal information is hereafter called an automatic use propriety setting-out port.

[0033](2) The administrator sets up the use propriety beforehand about the port which is not an automatic use propriety setting-out port.

[0034](3) The administrator sets up beforehand the address of the network management device which serves as a transmission destination of terminal information.

[0035](4) When a terminal is newly [network relay apparatus] connected in an automatic use propriety setting-out port etc., When terminal information should be transmitted, the identification key for discriminating terminals, such as a host name, from the frame which the automatic use propriety setting-out port received is detected, and it transmits to a network management device by making the identification key into terminal information.

[0036](5) Network relay apparatus sets up the port where the terminal is connected usable, when the information which shows an access permit from a network management device as a reply to transmission of terminal information is received.

[0037](6) Network relay apparatus sets up the port where the terminal is connected improper [use], when the information which shows an access inhibit from a network management device as a reply to transmission of terminal information is received.

[0038](7) When a network management device to a reply cannot be found after network relay apparatus transmitted terminal information to the network management device, it sets up use propriety as specified beforehand the sake [in this case].

[0039](8) Each setting detail (it is called the configuration information on network relay apparatus) set up by the above is stored in the memory 209. The junction circuit 207 uses the configuration information on the network relay apparatus 201 for communications processing since then.

[0040]The processing which the network management device 103 performs to below is shown.

[0041](1) It has the management table (what made a host name, and an access permit/inhibition information correspond, and registered it) 104 of each terminal and

the use propriety of a port in the inside, and setting out of this management table can be performed from on a management screen.

[0042](2) When the identification key (host name) which is terminal information is transmitted from network relay apparatus, a terminal is searched from the management table 104 and the information which shows an access permit or an access inhibit is replied to said network relay apparatus.

[0043](3) The contents of the inquiry (transmit terminal information) from network relay apparatus and the reply to the inquiry are recorded as a log. This log can be referred to from a management screen.

[0044]A more concrete flow is explained using drawing 1. Here, terminal information is a host name of a terminal.

[0045]The No. 1 port of the network relay apparatus 101 – the No. 4 port and the No. 1 port of the network relay apparatus 102, the No. 3 port – the No. 5 port shall be set as an automatic use propriety setting-out port. The No. 5 port of the network relay apparatus 101 and the No. 2 port of the network relay apparatus 102 shall be set up usable so that a self-opportunity and the terminal connected can communicate with a high order network.

[0046]The address of the network management device 103 shall be set to the network relay apparatus 101, 102 as an address of the network management device which serves as a transmission destination of terminal information.

[0047]Like [the network management device 103] a graphic display, setting out shall be beforehand made by the internal management table 104.

[0048]Now, a host name presupposes that the terminal 105 of red was connected to the No. 1 port of the network relay apparatus 101. If a frame is transmitted from the terminal 105, the MAC Address of the terminal 105 extracted from the frame will be registered into the filtering table (not shown) of the network relay apparatus 101. The network relay apparatus 101 detects the IP address of the terminal 105, searches a host name with the timing by DNS, and transmits the host name to the network management device 103 to it.

[0049]The network management device 103 searches the data corresponding to the host name which received from the management table 104. Since access is set to permission, as for the network management device 103, the host name red replies the information which shows an access permit to the network relay apparatus 101.

[0050]The network relay apparatus 101 which received the information which shows an access permit makes usable the No. 1 port where the terminal 105 is connected. Thereby, the terminal 105 can access a network now via the network relay apparatus

101.

[0051]Similarly, in the No. 3 port of the network relay apparatus 102, a host name is set up available, when the terminal 105 of red is connected to the No. 3 port of the network relay apparatus 102. That is, this terminal 105 can access a network, even if it connects with which port of which network relay apparatus.

[0052]Since access is set to prohibition at the management table 104 when the host name of the terminal 105 is blue, the information which shows an access inhibit from the network management device 103 to the inquiry from the network relay apparatus 101,102 is replied. Use of the port where the terminal 105 is connected of the network relay apparatus 101,102 which received the information which shows an access inhibit is made improper. Thereby, the terminal 105 cannot access a network via the network relay apparatus 101,102.

[0053]Since the host name applicable to the management table 104 is not registered when the host name of the terminal 105 is gray, the data of "others" of the management table 104 is referred to and access is set to the data with prohibition. The information which shows an access inhibit from the network management device 103 to the inquiry from the network relay apparatus 101,102 is replied. Since the network relay apparatus 101,102 makes improper use of the port where the terminal 105 is connected, the terminal 105 cannot access a network via the network relay apparatus 101,102. It can prevent making the terminal in which the unknown host name is set up by this access a network.

[0054]The contents of the inquiry and reply from the above network relay apparatus are recorded on the network management device 103, and an administrator can refer to the log from a management screen behind.

[0055]When communication with the network relay apparatus 101,102 and the network management device 103 is not completed and there is no reply to transmission of terminal information, the network relay apparatus 101,102 sets up the use propriety of a port as it was specified beforehand the sake [in such a case].

[0056]Thus, the configuration information on the set-up network relay apparatus is stored in the memory 209, and is used for communications processing by the junction circuit 207.

[0057]2) As shown in the second embodiment drawing 3, the network management system concerning this invention is provided with the following.

Two sets of network relay apparatus 101,102 concerning this invention.

The network management device 103 concerning this invention.

Network relay apparatus is a switching hub and has the internal configuration shown in

drawing 2, for example.

[0058]The processing which an administrator performs to below to the processing and network relay apparatus which the network relay apparatus of switching hub 201 grade performs is shown.

[0059](1) The administrator sets up whether it transmits to a network management device by making the user ID into terminal information, when a terminal user's user ID (identification information) is beforehand detected from the contents of the data received in the port for every port. The port which transmits the detected user ID is hereafter called an automatic use propriety setting-out port.

[0060](2) The administrator sets up the use propriety beforehand about the port which is not an automatic use propriety setting-out port.

[0061](3) The administrator sets up beforehand the address of the network management device which serves as a transmission destination of user ID.

[0062](4) Network relay apparatus transmits to a network management device by making the user ID into terminal information, when a terminal user's user ID is detected from the contents of the data received in a certain port.

[0063](5) Network relay apparatus sets up the port where the terminal is connected usable, when the information which shows an access permit from a network management device as a reply to transmission of user ID is received.

[0064](6) Network relay apparatus sets up the port where the terminal is connected improper [use], when the information which shows an access inhibit from a network management device as a reply to transmission of user ID is received.

[0065](7) When a network management device to a reply cannot be found after network relay apparatus transmitted user ID to the network management device, it sets up use propriety as specified beforehand the sake [in this case].

[0066](8) The configuration information on the network relay apparatus set up by the above is stored in the memory 209. The junction circuit 207 uses the configuration information on network relay apparatus for communications processing since then.

[0067]The processing which the network management device 103 performs to below is shown.

[0068](1) It has the management table (what made user ID, and an access permit/inhibition information correspond, and registered it) 104 of each user ID and the use propriety of a port in the inside, and setting out of this management table 104 can be performed from on a management screen.

[0069](2) When the user ID which is terminal information is transmitted from network relay apparatus, a terminal is searched from the management table 104 and the

information which shows an access permit or an access inhibit is replied to said network relay apparatus.

[0070](3) The contents of the inquiry from network relay apparatus and the reply to the inquiry are recorded as a log. This log can be referred to from a management screen.

[0071]A more concrete flow is explained using drawing 3.

[0072]The No. 1 port of the network relay apparatus 101 – the No. 4 port and the No. 1 port of the network relay apparatus 102, the No. 3 port – the No. 5 port shall be set as an automatic use propriety setting-out port. The No. 5 port of the network relay apparatus 101 and the No. 2 port of the network relay apparatus 102 shall be set up usable so that a self-opportunity and the terminal connected can communicate with a high order network.

[0073]The address of the network management device 103 shall be set to the network relay apparatus 101,102 as an address of the network management device which serves as a transmission destination of user ID.

[0074]Like [the network management device 103] a graphic display, setting out shall be beforehand made by the internal management table 104.

[0075]Now, it is assumed that the terminal 105 was connected to the No. 1 port of the network relay apparatus 101. Since the frame which has login information from the terminal 105 will be transmitted if a user with the user ID of a login name "Yamamoto" logs in to the terminal 105, The network relay apparatus 101 detects user ID "Yamamoto" from that frame, and transmits this user ID to the network management device 103.

[0076]The network management device 103 searches the data corresponding to the user ID which received from the management table 104. In this example, since access is set to permission to user ID "Yamamoto", the network management device 103 replies the information which shows an access permit to the network relay apparatus 101.

[0077]The network relay apparatus 101 which received the information which shows an access permit makes usable the No. 1 port where the terminal 105 is connected. Thereby, the terminal 105 can access a network now via the network relay apparatus 101.

[0078]If similarly a user with the user ID of "Yamamoto" logs in when the terminal 105 is connected to the No. 3 port of the network relay apparatus 102, the No. 3 port of the network relay apparatus 102 will be set up available.

[0079]Also when the user who has the user ID of "Yamamoto" in another terminal 106

connected to the No. 5 port of the network relay apparatus 102 logs in, the No. 5 port of the network relay apparatus 102 is set up available. That is, whether it uses which terminal or the user who uses user ID "Yamamoto" connects a terminal to which port of which network relay apparatus, he can access a network.

[0080]Since access is set to prohibition at the management table 104 when the user ID of the terminal 105 is "Kawaguti", the information which shows an access inhibit from the network management device 103 to the inquiry from the network relay apparatus 101,102 is replied. Use of the port where the terminal 105 is connected of the network relay apparatus 101,102 which received the information which shows an access inhibit is made improper. Thereby, the terminal 105 cannot access a network via the network relay apparatus 101,102.

[0081]Since the user ID applicable to the management table 104 is not registered when the user ID of the terminal 105 is "Yamada", Since the data of "others" of the management table 104 is referred to and access is set to the data with prohibition, the information which shows an access inhibit from the network management device 103 to the inquiry from the network relay apparatus 101,102 is replied. Since the network relay apparatus 101,102 makes improper use of the port where the terminal 105 is connected, the terminal 105 cannot access a network via the network relay apparatus 101,102. It can prevent making the terminal to which it logs in by this using unknown user ID access a network.

[0082]The contents of the inquiry and reply from the above network relay apparatus are recorded on the network management device 103, and an administrator can refer to the log from a management screen behind.

[0083]When communication with the network relay apparatus 101,102 and the network management device 103 is not completed and there is no reply to transmission of terminal information, the network relay apparatus 101,102 sets up the use propriety of a port as it was specified beforehand the sake [in such a case].

[0084]Thus, the configuration information on the set-up network relay apparatus is stored in the memory 209, and is used for communications processing by the junction circuit 207.

[0085]3) As shown in the third embodiment drawing 4, the network management system concerning this invention is provided with the following.

Two sets of network relay apparatus 101,102 concerning this invention.

The network management device 103 concerning this invention.

Network relay apparatus is a switching hub and has the internal configuration shown in drawing 2, for example.

[0086]The processing which an administrator performs to below to the processing and network relay apparatus which the network relay apparatus of switching hub 201 grade performs is shown.

[0087](1) Beforehand, the administrator sets up whether it transmits to a network management device by making the IP address of the terminal into terminal information, when a terminal is connected for every port. The port which transmits terminal information is hereafter called an automatic use propriety setting-out port.

[0088](2) The administrator sets up the use propriety beforehand about the port which is not an automatic use propriety setting-out port.

[0089](3) The administrator sets up beforehand the address of the network management device which serves as a transmission destination of an IP address.

[0090](4) When a MAC Address is newly [network relay apparatus] registered to a filtering table (not shown) etc., When the IP address of a terminal should be transmitted, the IP address of a terminal is detected from the frame which the automatic use propriety setting-out port received, and the IP address is transmitted to a network management device.

[0091](5) Network relay apparatus sets up the port where the terminal is connected usable, when the information which shows an access permit from a network management device as a reply to transmission of an IP address is received.

[0092](6) Network relay apparatus sets up the port where the terminal is connected improper [use], when the information which shows an access inhibit from a network management device as a reply to transmission of an IP address is received.

[0093](7) When a network management device to a reply cannot be found after network relay apparatus transmitted the IP address to the network management device, it sets up use propriety as specified beforehand the sake [in this case].

[0094](8) The configuration information on the network relay apparatus set up by the above is stored in the memory 209. The junction circuit 207 uses the configuration information on the network relay apparatus 201 for communications processing since then.

[0095]The processing which the network management device 103 performs to below is shown.

[0096](1) It has the management table (what made an IP address or IP subnet, and an access permit/inhibition information correspond, and registered it) 104 of each IP address (IP subnet ****) and the use propriety of a port in the inside, and setting out of this management table can be performed from on a management screen. Here, IP subnet can make a group an IP address and an effective-bits mask value, and can

specify two or more IP addresses using this IP subnet.

[0097](2) When an IP address is transmitted from network relay apparatus, an IP address is searched from the management table 104, and the information which shows an access permit or an access inhibit is replied to said network relay apparatus.

[0098](3) When the received IP address and the IP address in agreement are not registered into the management table 104, in IP subnet registered into the management table 104, Suiting IP subnet with the longest subnet mask length is searched, and the access permit/inhibition information corresponding to this IP subnet are replied to said network relay apparatus.

[0099](4) The contents of the inquiry from network relay apparatus and the reply to the inquiry are recorded as a log. This log can be referred to from a management screen.

[0100]A more concrete flow is explained using drawing 4.

[0101]The No. 1 port of the network relay apparatus 101 – the No. 4 port and the No. 1 port of the network relay apparatus 102, the No. 3 port – the No. 5 port shall be set as an automatic use propriety setting-out port. The No. 5 port of the network relay apparatus 101 and the No. 2 port of the network relay apparatus 102 shall be set up usable so that a self-opportunity and the terminal connected can communicate with a high order network.

[0102]The address of the network management device 103 shall be set to the network relay apparatus 101,102 as an address of the network management device which serves as a transmission destination of an IP address.

[0103]Like [the network management device 103] a graphic display, setting out shall be beforehand made by the internal management table 104.

[0104]Now, an IP address presupposes that the terminal 105 of 172.17.33.1 was connected to the No. 1 port of the network relay apparatus 101. If a frame is transmitted from the terminal 105, the MAC Address of the terminal 105 extracted from the frame will be registered into the filtering table of the network relay apparatus 101. To the timing, the network relay apparatus 101 detects an IP address, and transmits the IP address to the network management device 103.

[0105]The network management device 103 searches the data corresponding to the received IP address from the management table 104. Since access is set to permission, as for the network management device 103, IP address 172.17.33.1 replies the information which shows an access permit to the network relay apparatus 101.

[0106]The network relay apparatus 101 which received the information which shows an access permit makes usable the No. 1 port where the terminal 105 is connected.

Thereby, the terminal 105 can access a network now via the network relay apparatus 101.

[0107]Similarly, when this terminal 105 is connected to the No. 3 port of the network relay apparatus 102, the No. 3 port of the network relay apparatus 102 is set up available. That is, this terminal 105 can access a network, even if it connects with which port of which network relay apparatus.

[0108]Since access is set to prohibition at the management table 104 when the IP address of the terminal 105 is 172.17.33.2, the information which shows an access inhibit from the network management device 103 to the inquiry from the network relay apparatus 101,102 is replied. Use of the port where the terminal 105 is connected of the network relay apparatus 101,102 which received the information which shows an access inhibit is made improper. Thereby, the terminal 105 cannot access a network via the network relay apparatus 101,102.

[0109]When the IP address of the terminal 105 is 172.17.33.3, IP which is in agreement with the management table 104 is not registered. In this case, it is suiting IP subnet and the data of IP subnet with the longest subnet mask length is used. Therefore, since IP subnet of 172.17.33.*/24 suits this condition about 172.17.33.3, the information which shows a corresponding access permit is replied.

[0110]Similarly, when the IP address of the terminal 105 is 171.1.1.1, IP subnet 171.*.*.*/8 suit, and the information which shows an access permit is replied. When the IP address of the terminal 105 is 170.1.1.1, IP subnet *.*.*.*/0 suit and the information which shows an access inhibit is replied.

[0111]The contents of the inquiry and reply from the above network relay apparatus are recorded on the network management device 103, and an administrator can refer to the log from a management screen behind.

[0112]When communication with the network relay apparatus 101,102 and the network management device 103 is not completed etc., When there is no reply to transmission of an IP address, the network relay apparatus 101,102 sets up the use propriety of a port as it was specified beforehand the sake [in such a case].

[0113]Thus, the configuration information on the set-up network relay apparatus is stored in the memory 209, and is used for communications processing by the junction circuit 207.

[0114]4) As shown in the fourth embodiment drawing 5, the network management system concerning this invention is provided with the following.

Two sets of network relay apparatus 101,102 concerning this invention.

The network management device 103 concerning this invention.

Network relay apparatus is a switching hub and has the internal configuration shown in drawing 2, for example.

[0115]The processing which an administrator performs to below to the processing and network relay apparatus which the network relay apparatus of switching hub 201 grade performs is shown.

[0116](1) Beforehand, the administrator sets up whether it transmits to a network management device by making the MAC Address of the terminal into terminal information, when a terminal is connected for every port. The port which transmits terminal information is hereafter called an automatic use propriety setting-out port.

[0117](2) The administrator sets up the use propriety beforehand about the port which is not an automatic use propriety setting-out port.

[0118](3) The administrator sets up beforehand the address of the network management device which serves as a transmission destination of a MAC Address.

[0119](4) When a MAC Address is newly [network relay apparatus] registered to a filtering table (not shown) etc., When the MAC Address of a terminal should be transmitted, the MAC Address of a terminal is detected from the frame which the automatic use propriety setting-out port received, and the MAC Address is transmitted to a network management device.

[0120](5) Network relay apparatus sets up the port where the terminal is connected usable, when the information which shows an access permit from a network management device as a reply to transmission of a MAC Address is received.

[0121](6) Network relay apparatus sets up the port where the terminal is connected improper [use], when the information which shows an access inhibit from a network management device as a reply to transmission of a MAC Address is received.

[0122](7) When a network management device to a reply cannot be found after network relay apparatus transmitted the MAC Address to the network management device, it sets up use propriety as specified beforehand the sake [in this case].

[0123](8) The configuration information on the network relay apparatus set up by the above is stored in the memory 209. The junction circuit 207 uses the configuration information on the network relay apparatus 201 for communications processing since then.

[0124]The processing which the network management device 103 performs to below is shown.

[0125](1) It has the management table (what made a MAC Address, and an access permit/inhibition information correspond, and registered it) 104 of each MAC Address and the use propriety of a port in the inside, and setting out of this management table

can be performed from on a management screen.

[0126](2) When a MAC Address is transmitted from network relay apparatus, a MAC Address is searched from the management table 104, and the information which shows an access permit or an access inhibit is replied to said network relay apparatus.

[0127](3) The contents of the inquiry from network relay apparatus and the reply to the inquiry are recorded as a log. This log can be referred to from a management screen.

[0128]A more concrete flow is explained using drawing 5.

[0129]The No. 1 port of the network relay apparatus 101 – the No. 4 port and the No. 1 port of the network relay apparatus 102, the No. 3 port – the No. 5 port shall be set as an automatic use propriety setting-out port. The No. 5 port of the network relay apparatus 101 and the No. 2 port of the network relay apparatus 102 shall be set up usable so that a self-opportunity and the terminal connected can communicate with a high order network.

[0130]The address of the network management device 103 shall be set to the network relay apparatus 101, 102 as an address of the network management device which serves as a transmission destination of a MAC Address.

[0131]Like [the network management device 103] a graphic display, setting out shall be beforehand made by the internal management table 104.

[0132]Now, a MAC Address presupposes that the terminal 105 of 11:11:11:11:11:11 was connected to the No. 1 port of the network relay apparatus 101. If a frame is transmitted from the terminal 105, the MAC Address of the terminal 105 extracted from the frame will be registered into the filtering table of the network relay apparatus 101. The network relay apparatus 101 transmits the MAC Address to the network management device 103 to the timing.

[0133]The network management device 103 searches the data corresponding to the MAC Address which received from the management table 104. Since access is set to permission, as for the network management device 103, MAC Address 11:11:11:11:11:11 replies the information which shows an access permit to the network relay apparatus 101.

[0134]The network relay apparatus 101 which received the information which shows an access permit makes usable the No. 1 port where the terminal 105 is connected. Thereby, the terminal 105 can access a network now via the network relay apparatus 101.

[0135]Similarly, when this terminal 105 is connected to the No. 3 port of the network relay apparatus 102, the No. 3 port of the network relay apparatus 102 is set up

available. That is, this terminal 105 can access a network, even if it connects with which port of which network relay apparatus.

[0136]Since access is set as the management table 104 with prohibition when the MAC Address of the terminal 105 is 22:22:22:22:22:22, The information which shows an access inhibit from the network management device 103 to the inquiry from the network relay apparatus 101,102 is replied. Use of the port where the terminal 105 is connected of the network relay apparatus 101,102 which received the information which shows an access inhibit is made improper. Thereby, the terminal 105 cannot access a network via the network relay apparatus 101,102.

[0137]Since the MAC Address applicable to the management table 104 is not registered when the MAC Address of the terminal 105 is 44:44:44:44:44:44, Since the data of "others" of the management table 104 is referred to and access is set to the data with prohibition, the information which shows an access inhibit from the network management device 103 to the inquiry from the network relay apparatus 101,102 is replied. Since the network relay apparatus 101,102 makes improper use of the port where the terminal 105 is connected, the terminal 105 cannot access a network via the network relay apparatus 101,102. It can prevent making the terminal of an unknown MAC Address access a network by this.

[0138]The contents of the inquiry and reply from the above network relay apparatus are recorded on the network management device 103, and an administrator can refer to the log from a management screen behind.

[0139]When communication with the network relay apparatus 101,102 and the network management device 103 is not completed etc., When there is no reply to transmission of a MAC Address, the network relay apparatus 101,102 sets up the use propriety of a port as it was specified beforehand the sake [in such a case].

[0140]Thus, the configuration information on the set-up network relay apparatus is stored in the memory 209, and is used for communications processing by the junction circuit 207.

[0141]

[Effect of the Invention]This invention demonstrates the outstanding effect like the next.

[0142](1) Only the terminal attested by terminal information, such as a host name (identification key), user ID, an IP address, and a MAC Address, can access a network now, and network security can be secured.

[0143](2) Integrated management of the use propriety of a port can be carried out for every user using every terminal or a terminal.

[0144](3) The information on the splicing terminal for every port and the log of use propriety setting out can be referred to.

[0145](4) The address of the network management device which manages use propriety can be set up freely.

[0146](5) Setting out of the use propriety of the port by this invention cannot be used in all the ports, either.

[0147](6) It can be set up whether setting out of the use propriety of the port by this invention is used for every port.

[0148](7) When there is no reply from a network management device to transmission of terminal information, it can be specified beforehand whether what we do with the use propriety of the port where the terminal is connected.

[Brief Description of the Drawings]

[Drawing 1]It is a lineblock diagram of a network management system showing a first embodiment of this invention.

[Drawing 2]It is an internal configuration figure of a switching hub showing the embodiment of the network relay apparatus of this invention.

[Drawing 3]It is a lineblock diagram of a network management system showing a second embodiment of this invention.

[Drawing 4]It is a lineblock diagram of a network management system showing a third embodiment of this invention.

[Drawing 5]It is a lineblock diagram of a network management system showing a fourth embodiment of this invention.

[Description of Notations]

101,102 network relay apparatus

103 Network management device

104 Management table

105 Terminal

[Translation done.]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-141916

(P2002-141916A)

(43)公開日 平成14年5月17日 (2002.5.17)

(51)Int.Cl.⁷

H 0 4 L 12/28
12/44

識別記号

F I

H 0 4 L 11/00

テ-マコ-ト(参考)

3 1 0 D 5 K 0 3 3
3 4 0

審査請求 未請求 請求項の数23 O L (全 10 頁)

(21)出願番号

特願2000-337266(P2000-337266)

(22)出願日

平成12年10月31日 (2000.10.31)

(71)出願人 000005120

日立電線株式会社

東京都千代田区大手町一丁目6番1号

(72)発明者 平岡 大樹

茨城県日立市砂沢町880番地 日立電線株式会社高砂工場内

(74)代理人 100068021

弁理士 綱谷 信雄

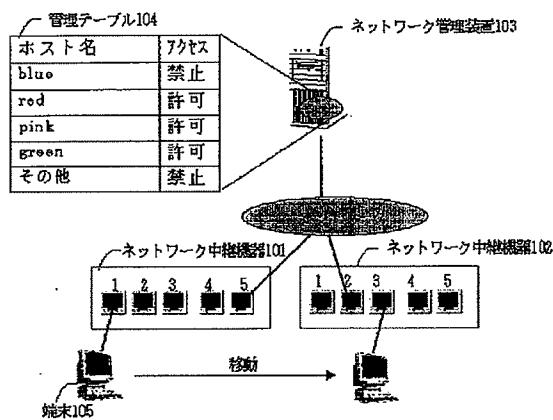
F ターム(参考) 5K033 BA04 BA08 DA05 DA15 DB12
DB14 DB17 DB18 DB20 EA07
EC01

(54)【発明の名称】 ネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置

(57)【要約】

【課題】 セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置を提供する。

【解決手段】 ネットワーク中継機器101より接続されている端末105の情報をネットワーク管理装置103に送信し、そのネットワーク管理装置103が前記端末情報に応じてアクセス許可/禁止を示す情報をネットワーク中継機器101に返信し、ネットワーク中継機器101が前記アクセス許可/禁止情報に基づいて端末105を接続しているポートを使用可能/使用不可に設定する。ネットワーク管理装置103が管理する端末情報に応じてネットワーク中継機器101のポートの使用可否が設定されるので、正当な端末の利用を妨げることなくセキュリティが確保される。



【特許請求の範囲】

【請求項1】 ネットワーク中継機器より接続されている端末の情報をネットワーク管理装置に送信し、そのネットワーク管理装置が前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信し、前記ネットワーク中継機器が前記アクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定することを特徴とするネットワーク管理システム。

【請求項2】 前記端末情報は、当該端末を使用しているユーザの識別情報であることを特徴とする請求項1記載のネットワーク管理システム。

【請求項3】 前記端末情報は、当該端末のホスト名であることを特徴とする請求項1記載のネットワーク管理システム。

【請求項4】 前記端末情報は、当該端末のIPアドレスであることを特徴とする請求項1記載のネットワーク管理システム。

【請求項5】 前記端末情報は、当該端末のMACアドレスであることを特徴とする請求項1記載のネットワーク管理システム。

【請求項6】 ネットワーク中継機器において、接続されている端末の情報をネットワーク管理装置に送信する機能を備えたことを特徴とするネットワーク中継機器。

【請求項7】 前記端末情報の送信に対する返信として前記ネットワーク管理装置からアクセス許可／禁止を示す情報を受信した場合、このアクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定する機能を備えたことを特徴とする請求項6記載のネットワーク中継機器。

【請求項8】 前記端末情報をネットワーク管理装置に送信するポートと前記端末情報をネットワーク管理装置に送信しないポートとの設定がポート毎にできる機能を備えたことを特徴とする請求項6又は7記載のネットワーク中継機器。

【請求項9】 前記端末情報をネットワーク管理装置に送信しないポートに対し任意にポートの使用可否が設定できる機能を備えたことを特徴とする請求項8記載のネットワーク中継機器。

【請求項10】 前記端末情報をどのネットワーク管理装置に送信するかを指定しておくことができる機能を備えたことを特徴とする請求項6～9いずれか記載のネットワーク中継機器。

【請求項11】 前記端末情報の送信に対する前記ネットワーク管理装置からの返信がなかった場合、端末が接続されているポートの使用可否が予め設定できる機能を備えたことを特徴とする請求項6～10いずれか記載のネットワーク中継機器。

【請求項12】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末を使用しているユー

ザの識別情報をあることを特徴とする請求項6～11いずれか記載のネットワーク中継機器。

【請求項13】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のホスト名であることを特徴とする請求項6～11のいずれか記載のネットワーク中継機器。

【請求項14】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のIPアドレスであることを特徴とする請求項6～11いずれか記載のネットワーク中継機器。

【請求項15】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のMACアドレスであることを特徴とする請求項6～11いずれか記載のネットワーク中継機器。

【請求項16】 ネットワーク管理装置において、ネットワーク中継機器から端末の情報を受信した場合、前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信する機能を備えたことを特徴とするネットワーク管理装置。

【請求項17】 前記ネットワーク中継機器に返信するべきアクセス許可／禁止を示す情報と前記端末情報との対応を管理できる機能を備えたことを特徴とする請求項16記載のネットワーク管理装置。

【請求項18】 前記端末情報は、当該端末を使用しているユーザの識別情報であることを特徴とする請求項16又は17記載のネットワーク管理装置。

【請求項19】 前記端末情報は、当該端末のホスト名であることを特徴とする請求項16又は17記載のネットワーク管理装置。

【請求項20】 前記端末情報は、当該端末のIPアドレスであることを特徴とする請求項16又は17記載のネットワーク管理装置。

【請求項21】 前記端末情報は、当該端末のMACアドレスであることを特徴とする請求項16又は17記載のネットワーク管理装置。

【請求項22】 IPアドレスと有効ビットマスク値とを組として複数のIPアドレスを指定するIPサブネットを用い、このIPサブネットとアクセス許可／禁止情報との対応を定義しておき、この定義に照らして前記アクセス許可／禁止情報と前記端末のIPアドレスとの対応を管理する機能を備えたことを特徴とする請求項20記載のネットワーク管理装置。

【請求項23】 前記ネットワーク中継機器からの送信及びその送信に対する返信の内容をログとして記録し、このログを管理画面から参照できる機能を備えたことを特徴とする請求項16～22いずれか記載のネットワーク管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワーク中継

機器を用いたネットワーク管理システムに係り、特に、セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置に関するものである。

【0002】

【従来の技術】多くのネットワーク中継機器は、ポートの使用可否の設定機能を備えている。ポートを使用不可に設定すると、そのポートに接続されたネットワーク機器は前記ネットワーク中継機器を介して通信を行うことができない。

【0003】

【発明が解決しようとする課題】ネットワーク上に設置されているネットワーク中継機器に、どの端末を接続しても、ポートが使用可能に設定されていれば、その端末は前記ネットワーク中継機器を介して通信を行うことができる。仮に、悪意を持った外部からの侵入者の端末でも同様に通信を行うことができる。侵入者の端末がネットワークにアクセスできないようポートを使用不可に設定すると、本来、ネットワークにアクセスが許されるべき端末をもネットワークにアクセスさせないことになってしまう。このように、従来のネットワーク中継機器を用いたネットワーク管理システムではセキュリティの確保が難しい。

【0004】そこで、本発明の目的は、上記課題を解決し、セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置を提供することにある。

【0005】

【課題を解決するための手段】上記目的を達成するためには本発明のネットワーク管理装置は、ネットワーク中継機器より接続されている端末の情報をネットワーク管理装置に送信し、そのネットワーク管理装置が前記端末情報を応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信し、前記ネットワーク中継機器が前記アクセス許可／禁止情報を基づいて端末を接続しているポートを使用可能／使用不可に設定するものである。

【0006】前記端末情報は、当該端末を使用しているユーザの識別情報であってもよい。

【0007】前記端末情報は、当該端末のホスト名であってもよい。

【0008】前記端末情報は、当該端末のIPアドレスであってもよい。

【0009】前記端末情報は、当該端末のMACアドレスであってもよい。

【0010】また、本発明のネットワーク中継機器は、接続されている端末の情報をネットワーク管理装置に送信する機能を備えたものである。

【0011】前記端末情報の送信に対する返信として前記ネットワーク管理装置からアクセス許可／禁止を示す

情報を受信した場合、このアクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定する機能を備えてもよい。

【0012】前記端末情報をネットワーク管理装置に送信するポートと前記端末情報をネットワーク管理装置に送信しないポートとの設定がポート毎にできる機能を備えてもよい。

【0013】前記端末情報をネットワーク管理装置に送信しないポートに対し任意にポートの使用可否が設定できる機能を備えてもよい。

【0014】前記端末情報をどのネットワーク管理装置に送信するかを指定しておくことができる機能を備えてもよい。

【0015】前記端末情報の送信に対する前記ネットワーク管理装置からの返信がなかった場合、端末が接続されているポートの使用可否が予め設定できる機能を備えてもよい。

【0016】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末を使用しているユーザの識別情報であってもよい。

【0017】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のホスト名であってもよい。

【0018】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のIPアドレスであってもよい。

【0019】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のMACアドレスであってもよい。

【0020】また、本発明のネットワーク管理装置は、ネットワーク中継機器から端末の情報を受信した場合、前記端末情報を応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信する機能を備えたものである。

【0021】前記ネットワーク中継機器に返信するべきアクセス許可／禁止を示す情報と前記端末情報との対応を管理できる機能を備えてもよい。

【0022】前記端末情報は、当該端末を使用しているユーザの識別情報であってもよい。

【0023】前記端末情報は、当該端末のホスト名であってもよい。

【0024】前記端末情報は、当該端末のIPアドレスであってもよい。

【0025】前記端末情報は、当該端末のMACアドレスであってもよい。

【0026】IPアドレスと有効ビットマスク値を組として複数のIPアドレスを指定するIPサブネットを用い、このIPサブネットとアクセス許可／禁止情報との対応を定義しておき、この定義に照らして前記アクセス許可／禁止情報と前記端末のIPアドレスとの対応を

管理する機能を備えてもよい。

【0027】前記ネットワーク中継機器からの送信及びその送信に対する返信の内容をログとして記録し、このログを管理画面から参照できる機能を備えてもよい。

【0028】

【発明の実施の形態】以下、本発明の実施形態を添付図面に基づいて詳述する。

【0029】1) 第一の実施形態

図1に示されるように、本発明に係るネットワーク管理システムは、本発明に係る2台のネットワーク中継機器101、102と、本発明に係るネットワーク管理装置103とを有する。ネットワーク中継機器は、例えば、スイッチングハブである。

【0030】図2に示されるように、スイッチングハブ201は、1番～5番ポート202～206、中継回路207、プロセッサ208、メモリ209等から構成されている。

【0031】以下に、スイッチングハブ201等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0032】(1) 管理者は、予めポート毎に、端末が接続された場合に、その端末の情報をネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0033】(2) 管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0034】(3) 管理者は、端末情報の送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0035】(4) ネットワーク中継機器は、自動使用可否設定ポートに新たに端末が接続された場合など、端末情報を送信するべき際、自動使用可否設定ポートが受信したフレームからホスト名等の端末を識別するための識別キーを検出し、その識別キーを端末情報としてネットワーク管理装置に送信する。

【0036】(5) ネットワーク中継機器は、端末情報の送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0037】(6) ネットワーク中継機器は、端末情報の送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0038】(7) ネットワーク中継機器は、ネットワーク管理装置に端末情報を送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【0039】(8) 以上によって設定された各設定内容(ネットワーク中継機器の構成情報と呼ぶ)はメモリ209に格納される。爾後、中継回路207は、ネットワ

10

ーク中継機器201の構成情報を通信処理に使用する。

【0040】以下、ネットワーク管理装置103が行う処理を示す。

【0041】(1) 各端末とポートの使用可否との管理テーブル(ホスト名とアクセス許可／禁止情報を対応させて登録したもの)104を内部に持つており、管理画面上からこの管理テーブルの設定ができる。

【0042】(2) ネットワーク中継機器から端末情報である識別キー(ホスト名)が送信された場合、管理テーブル104から端末を検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0043】(3) ネットワーク中継機器からの問い合わせ(端末情報を送信すること)及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面上から参照できる。

【0044】図1を用いて、より具体的な流れを説明する。ここでは、端末情報は端末のホスト名である。

20

【0045】ネットワーク中継機器101の1番ポート～4番ポート及びネットワーク中継機器102の1番ポート、3番ポート～5番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器101の5番ポート及びネットワーク中継機器102の2番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【0046】また、ネットワーク中継機器101、102には、端末情報の送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置103のアドレスが設定されているものとする。

30

【0047】ネットワーク管理装置103には、図示のように、予め内部の管理テーブル104に設定がなされているものとする。

【0048】いま、ホスト名がredの端末105がネットワーク中継機器101の1番ポートに接続されたとする。端末105からフレームが送信されると、ネットワーク中継機器101のフィルタリングテーブル(図示せず)にフレームから抽出した端末105のMACアドレスが登録される。そのタイミングでネットワーク中継機器101は、端末105のIPアドレスを検出し、DNSによりホスト名を検索し、そのホスト名をネットワーク管理装置103に送信する。

40

【0049】ネットワーク管理装置103は、受信したホスト名に対応したデータを管理テーブル104から検索する。ホスト名redは、アクセスが許可と設定されているので、ネットワーク管理装置103は、アクセス許可を示す情報をネットワーク中継機器101に返信する。

50

【0050】アクセス許可を示す情報を受信したネットワーク中継機器101は、端末105が接続されている

1番ポートを使用可能にする。これにより、端末105は、ネットワーク中継機器101を介してネットワークにアクセスすることができるようになる。

【0051】同様に、ホスト名がredの端末105がネットワーク中継機器102の3番ポートに接続された場合も、ネットワーク中継機器102の3番ポートは利用可能に設定される。つまり、この端末105は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができるようになる。

【0052】端末105のホスト名がblueの場合、管理テーブル104にアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受けたネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にする。これにより、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。

【0053】端末105のホスト名がgrayの場合、管理テーブル104に該当するホスト名が登録されていないため、管理テーブル104の“その他”的データが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。ネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にするので、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。これにより、不明なホスト名が設定されている端末をネットワークにアクセスさせることを防ぐことができる。

【0054】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置103に記録され、後に管理者がそのログを管理画面から参照することができる。

【0055】ネットワーク中継機器101、102とネットワーク管理装置103との通信ができなかった場合など、端末情報の送信に対する返信がなかった場合、ネットワーク中継機器101、102は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0056】このようにして設定されたネットワーク中継機器の構成情報は、メモリ209に格納され、中継回路207によって通信処理に使用される。

【0057】2) 第二の実施形態

図3に示されるように、本発明に係るネットワーク管理システムは、本発明に係る2台のネットワーク中継機器101、102と、本発明に係るネットワーク管理装置103とを有する。ネットワーク中継機器は、例えば、

スイッチングハブであり、図2に示した内部構成を有する。

【0058】以下に、スイッチングハブ201等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0059】(1) 管理者は、予めポート毎に、そのポートで受信したデータの内容から端末使用者のユーザID(識別情報)を検知した場合にそのユーザIDを端末情報としてネットワーク管理装置に送信するかどうかを設定しておく。検知したユーザIDを送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0060】(2) 管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0061】(3) 管理者は、ユーザIDの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0062】(4) ネットワーク中継機器は、あるポートで受信したデータの内容から端末使用者のユーザIDを検知した場合、そのユーザIDを端末情報としてネットワーク管理装置に送信する。

【0063】(5) ネットワーク中継機器は、ユーザIDの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0064】(6) ネットワーク中継機器は、ユーザIDの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0065】(7) ネットワーク中継機器は、ネットワーク管理装置にユーザIDを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあった通りに使用可否の設定を行う。

【0066】(8) 以上によって設定されたネットワーク中継機器の構成情報はメモリ209に格納される。爾後、中継回路207は、ネットワーク中継機器の構成情報を通信処理に使用する。

【0067】以下に、ネットワーク管理装置103が行う処理を示す。

【0068】(1) 各ユーザIDとポートの使用可否との管理テーブル(ユーザIDとアクセス許可/禁止情報を対応させて登録したもの)104を内部に持つておらず、管理画面上からこの管理テーブル104の設定ができる。

【0069】(2) ネットワーク中継機器から端末情報であるユーザIDが送信された場合、管理テーブル104から端末を検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0070】(3) ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとし

て記録する。このログは、管理画面から参照できる。

【0071】図3を用いて、より具体的な流れを説明する。

【0072】ネットワーク中継機器101の1番ポート～4番ポート及びネットワーク中継機器102の1番ポート、3番ポート～5番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器101の5番ポート及びネットワーク中継機器102の2番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【0073】また、ネットワーク中継機器101、102には、ユーザIDの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置103のアドレスが設定されているものとする。

【0074】ネットワーク管理装置103には、図示のように、予め内部の管理テーブル104に設定がなされているものとする。

【0075】いま、端末105がネットワーク中継機器101の1番ポートに接続されていたとする。ログイン名“Yamamoto”的ユーザIDを持つユーザが端末105にログインすると、端末105からログイン情報を持つフレームが送信されるので、ネットワーク中継機器101は、そのフレームからユーザID“Yamamoto”を検出し、このユーザIDをネットワーク管理装置103に送信する。

【0076】ネットワーク管理装置103は、受信したユーザIDに対応したデータを管理テーブル104から検索する。この例では、ユーザID“Yamamoto”に対しアクセスが許可と設定されているので、ネットワーク管理装置103は、アクセス許可を示す情報をネットワーク中継機器101に返信する。

【0077】アクセス許可を示す情報を受信したネットワーク中継機器101は、端末105が接続されている1番ポートを使用可能にする。これにより、端末105は、ネットワーク中継機器101を介してネットワークにアクセスすることができるようになる。

【0078】同様に、端末105がネットワーク中継機器102の3番ポートに接続された場合も、“Yamamoto”的ユーザIDを持つユーザがログインすれば、ネットワーク中継機器102の3番ポートは利用可能に設定される。

【0079】また、ネットワーク中継機器102の5番ポートに接続された別の端末106に“Yamamoto”的ユーザIDを持つユーザがログインした場合も、ネットワーク中継機器102の5番ポートは利用可能に設定される。つまり、ユーザID“Yamamoto”を使用するユーザは、どの端末を使用しても、また端末をどのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることにな

る。

【0080】端末105のユーザIDが“Kawagi”的場合、管理テーブル104にアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にする。これにより、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。

【0081】端末105のユーザIDが“Yamada”的場合、管理テーブル104に該当するユーザIDが登録されていないため、管理テーブル104の“その他”的データが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。ネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にするので、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。これにより、不明なユーザIDを使用してログインされる端末をネットワークにアクセスさせることを防ぐことができる。

【0082】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置103に記録され、後に管理者がそのログを管理画面から参照することができる。

【0083】ネットワーク中継機器101、102とネットワーク管理装置103との通信ができなかった場合など、端末情報の送信に対する返信がなかった場合、ネットワーク中継機器101、102は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0084】このようにして設定されたネットワーク中継機器の構成情報は、メモリ209に格納され、中継回路207によって通信処理に使用される。

【0085】3) 第三の実施形態

40 図4に示されるように、本発明に係るネットワーク管理システムは、本発明に係る2台のネットワーク中継機器101、102と、本発明に係るネットワーク管理装置103とを有する。ネットワーク中継機器は、例えば、スイッチングハブであり、図2に示した内部構成を有する。

【0086】以下に、スイッチングハブ201等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0087】(1) 管理者は、予めポート毎に、端末が接続された場合に、その端末のIPアドレスを端末情報

としてネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0088】(2)管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0089】(3)管理者は、IPアドレスの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0090】(4)ネットワーク中継機器は、フィルタリングテーブル(図示せず)に新たにMACアドレスが登録される場合など、端末のIPアドレスを送信すべき際、自動使用可否設定ポートが受信したフレームから端末のIPアドレスを検出し、そのIPアドレスをネットワーク管理装置に送信する。

【0091】(5)ネットワーク中継機器は、IPアドレスの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0092】(6)ネットワーク中継機器は、IPアドレスの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0093】(7)ネットワーク中継機器は、ネットワーク管理装置にIPアドレスを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【0094】(8)以上によって設定されたネットワーク中継機器の構成情報はメモリ209に格納される。爾後、中継回路207は、ネットワーク中継機器201の構成情報を通信処理に使用する。

【0095】以下に、ネットワーク管理装置103が行う処理を示す。

【0096】(1)各IPアドレス(IPサブネット含む)とポートの使用可否との管理テーブル(IPアドレス又はIPサブネットとアクセス許可/禁止情報を対応させて登録したもの)104を内部に持っており、管理画面上からこの管理テーブルの設定ができる。ここで、IPサブネットは、IPアドレスと有効ビットマスク値とを組とするものであり、このIPサブネットを用いて複数のIPアドレスを指定することができる。

【0097】(2)ネットワーク中継機器からIPアドレスが送信された場合、管理テーブル104からIPアドレスを検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0098】(3)受信したIPアドレスと一致するIPアドレスが管理テーブル104に登録されていない場合、管理テーブル104に登録されているIPサブネットの中で、適合する最もサブネットマスク長が長いIPサブネットを検索し、このIPサブネットに対応するア

クセス許可/禁止情報を前記ネットワーク中継機器に返信する。

【0099】(4)ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面から参照できる。

【0100】図4を用いて、より具体的な流れを説明する。

【0101】ネットワーク中継機器101の1番ポート～4番ポート及びネットワーク中継機器102の1番ポート、3番ポート～5番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器101の5番ポート及びネットワーク中継機器102の2番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【0102】また、ネットワーク中継機器101、102には、IPアドレスの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置103のアドレスが設定されているものとする。

【0103】ネットワーク管理装置103には、図示のように、予め内部の管理テーブル104に設定がなされているものとする。

【0104】いま、IPアドレスが172.17.33.1の端末105がネットワーク中継機器101の1番ポートに接続されたとする。端末105からフレームが送信されると、ネットワーク中継機器101のフィルタリングテーブルにフレームから抽出した端末105のMACアドレスが登録される。そのタイミングでネットワーク中継機器101は、IPアドレスを検出し、そのIPアドレスをネットワーク管理装置103に送信する。

【0105】ネットワーク管理装置103は、受信したIPアドレスに対応したデータを管理テーブル104から検索する。IPアドレス172.17.33.1は、アクセスが許可と設定されているので、ネットワーク管理装置103は、アクセス許可を示す情報をネットワーク中継機器101に返信する。

【0106】アクセス許可を示す情報を受信したネットワーク中継機器101は、端末105が接続されている1番ポートを使用可能にする。これにより、端末105は、ネットワーク中継機器101を介してネットワークにアクセスすることができるようになる。

【0107】同様に、この端末105がネットワーク中継機器102の3番ポートに接続された場合も、ネットワーク中継機器102の3番ポートは利用可能に設定される。つまり、この端末105は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができるようになる。

【0108】端末105のIPアドレスが172.17.33.2の場合、管理テーブル104にアクセスが

禁止と設定されているので、ネットワーク中継機器101, 102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器101, 102は、端末105が接続されているポートを使用不可にする。これにより、端末105は、ネットワーク中継機器101, 102を介してネットワークにアクセスすることができない。

【0109】端末105のIPアドレスが172.17.33.3の場合、管理テーブル104に一致するIPが登録されていない。この場合、適合するIPサブネットであって最もサブネットマスク長が長いIPサブネットのデータが使用される。従って、172.17.33.3については、172.17.33.*/24のIPサブネットがこの条件に適合するので、対応するアクセス許可を示す情報が返信される。

【0110】同様に、端末105のIPアドレスが171.1.1.1の場合、IPサブネット171.*.*.*/8が適合し、アクセス許可を示す情報が返信される。端末105のIPアドレスが170.1.1.1の場合は、IPサブネット*.*.*.*/0が適合し、アクセス禁止を示す情報が返信される。

【0111】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置103に記録され、後に管理者がそのログを管理画面から参照することができる。

【0112】ネットワーク中継機器101, 102とネットワーク管理装置103との通信ができなかった場合など、IPアドレスの送信に対する返信がなかった場合、ネットワーク中継機器101, 102は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0113】このようにして設定されたネットワーク中継機器の構成情報は、メモリ209に格納され、中継回路207によって通信処理に使用される。

【0114】4) 第四の実施形態
図5に示されるように、本発明に係るネットワーク管理システムは、本発明に係る2台のネットワーク中継機器101, 102と、本発明に係るネットワーク管理装置103とを有する。ネットワーク中継機器は、例えば、スイッチングハブであり、図2に示した内部構成を有する。

【0115】以下に、スイッチングハブ201等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0116】(1) 管理者は、予めポート毎に、端末が接続された場合に、その端末のMACアドレスを端末情報としてネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0117】(2) 管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0118】(3) 管理者は、MACアドレスの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0119】(4) ネットワーク中継機器は、フィルタリングテーブル(図示せず)に新たにMACアドレスが登録される場合など、端末のMACアドレスを送信するべき際、自動使用可否設定ポートが受信したフレームから端末のMACアドレスを検出し、そのMACアドレスをネットワーク管理装置に送信する。

【0120】(5) ネットワーク中継機器は、MACアドレスの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0121】(6) ネットワーク中継機器は、MACアドレスの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0122】(7) ネットワーク中継機器は、ネットワーク管理装置にMACアドレスを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【0123】(8) 以上によって設定されたネットワーク中継機器の構成情報はメモリ209に格納される。爾後、中継回路207は、ネットワーク中継機器201の構成情報を通信処理に使用する。

【0124】以下に、ネットワーク管理装置103が行う処理を示す。

【0125】(1) 各MACアドレスとポートの使用可否との管理テーブル(MACアドレスとアクセス許可/禁止情報とを対応させて登録したもの)104を内部に持つておらず、管理画面上からこの管理テーブルの設定ができる。

【0126】(2) ネットワーク中継機器からMACアドレスが送信された場合、管理テーブル104からMACアドレスを検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0127】(3) ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面上から参照できる。

【0128】図5を用いて、より具体的な流れを説明する。

【0129】ネットワーク中継機器101の1番ポート～4番ポート及びネットワーク中継機器102の1番ポート、3番ポート～5番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器101の5番ポート及びネットワーク中継機器102の2番ポートは、自機及び接続される端末が上位ネット

ワークと通信できるように使用可能に設定されているものとする。

【0130】また、ネットワーク中継機器101, 102には、MACアドレスの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置103のアドレスが設定されているものとする。

【0131】ネットワーク管理装置103には、図示のように、予め内部の管理テーブル104に設定がなされているものとする。

【0132】いま、MACアドレスが11:11:11:11:11:11の端末105がネットワーク中継機器101の1番ポートに接続されたとする。端末105からフレームが送信されると、ネットワーク中継機器101のフィルタリングテーブルにフレームから抽出した端末105のMACアドレスが登録される。そのタイミングでネットワーク中継機器101は、そのMACアドレスをネットワーク管理装置103に送信する。

【0133】ネットワーク管理装置103は、受信したMACアドレスに対応したデータを管理テーブル104から検索する。MACアドレス11:11:11:11:11:11は、アクセスが許可と設定されているので、ネットワーク管理装置103は、アクセス許可を示す情報をネットワーク中継機器101に返信する。

【0134】アクセス許可を示す情報を受信したネットワーク中継機器101は、端末105が接続されている1番ポートを使用可能にする。これにより、端末105は、ネットワーク中継機器101を介してネットワークにアクセスすることができるようになる。

【0135】同様に、この端末105がネットワーク中継機器102の3番ポートに接続された場合も、ネットワーク中継機器102の3番ポートは利用可能に設定される。つまり、この端末105は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【0136】端末105のMACアドレスが22:22:22:22:22:22の場合、管理テーブル104にアクセスが禁止と設定されているので、ネットワーク中継機器101, 102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器101, 102は、端末105が接続されているポートを使用不可にする。これにより、端末105は、ネットワーク中継機器101, 102を介してネットワークにアクセスすることができない。

【0137】端末105のMACアドレスが44:44:44:44:44:44の場合、管理テーブル104に該当するMACアドレスが登録されていないため、管理テーブル104の“その他”的データが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器101, 102からの問い合わせ

に対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。ネットワーク中継機器101, 102は、端末105が接続されているポートを使用不可にするので、端末105は、ネットワーク中継機器101, 102を介してネットワークにアクセスすることができない。これにより、不明なMACアドレスの端末をネットワークにアクセスさせることを防ぐことができる。

【0138】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置103に記録され、後に管理者がそのログを管理画面から参照することができる。

【0139】ネットワーク中継機器101, 102とネットワーク管理装置103との通信ができなかった場合など、MACアドレスの送信に対する返信がなかった場合、ネットワーク中継機器101, 102は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0140】このようにして設定されたネットワーク中継機器の構成情報は、メモリ209に格納され、中継回路207によって通信処理に使用される。

【0141】

【発明の効果】本発明は次の如き優れた効果を発揮する。

【0142】(1) ホスト名(識別キー)、ユーザID、IPアドレス、MACアドレス等の端末情報によって認証されている端末のみがネットワークにアクセスできるようになり、ネットワークのセキュリティを確保することができる。

【0143】(2) 各端末毎あるいは端末を利用するユーザ毎にポートの利用可否を統合管理することができる。

【0144】(3) ポート毎の接続端末の情報や利用可否設定のログを参照することができる。

【0145】(4) 利用可否を管理するネットワーク管理装置のアドレスを自由に設定することができる。

【0146】(5) 本発明によるポートの利用可否の設定を全ポートで使用しないこともできる。

【0147】(6) 本発明によるポートの利用可否の設定をポート毎に使用するか否かを設定できる。

【0148】(7) 端末情報の送信に対するネットワーク管理装置からの返信がなかった場合に端末が接続されているポートの使用可否をどうするかを予め指定しておくことができる。

【図面の簡単な説明】

【図1】本発明の第一の実施形態を示すネットワーク管理システムの構成図である。

【図2】本発明のネットワーク中継機器の実施形態を示すスイッチングハブの内部構成図である。

【図3】本発明の第二の実施形態を示すネットワーク管理システムの構成図である。

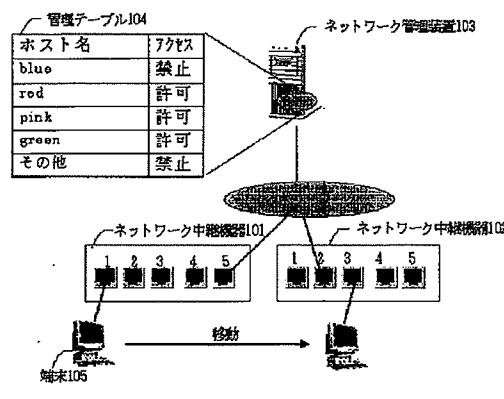
【図4】本発明の第三の実施形態を示すネットワーク管理システムの構成図である。

【図5】本発明の第四の実施形態を示すネットワーク管理システムの構成図である。

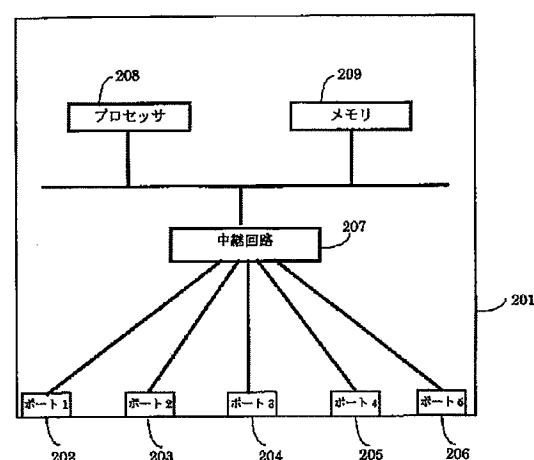
【符号の説明】

*

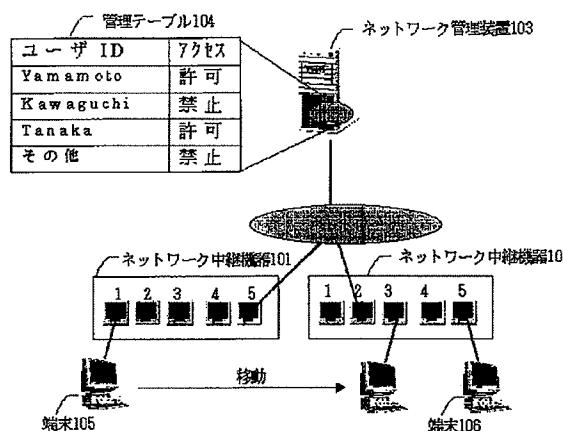
【図1】



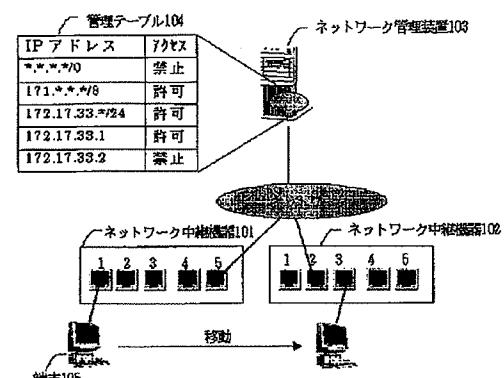
【図2】



【図3】



【図4】



【図5】

